(1)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105612
(43)Dat of publication of application : 24.04.1998

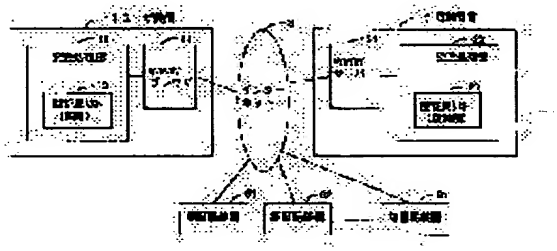
(51)Int.Cl. G06F 17/60

(21)Application number : 08-260757
(22)Date of filing : 01.10.1996

(71)Applicant : FUJITSU LTD
(72)Inventor : NAKAMURA KIMIHARU
EYA TAMEYUKI
KANDA YASUNORI

(54) AUTHENTIFICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To allow a user to easily select an authentification station out of plural authentification stations by xecuting the electronic settlement of accounts while using a k y issued by a common authentification station included in the list of authentification stations contracted by the owner of a s rver and the list of authentification stations contracted by the user of cliend equipment.
SOLUTION: Respecive authentification station devices 61-6n issue respectively independent public keys to contracted users and shops. Therefore, when a certain user or shop respectively contracts two authentification station devices 61 and 6n, that user or ship is to have two public keys respectively. Accordingly, when the user executes ordering processing through a network to a certain shop, without confirming whether the user himself contracts the same certification station device or not, the electronic settlement of accounts is nabled by using the public key issued by the mutually common certification station device while utilizing two certification station lists 13 and 23. Thus, the user can easily select the authentification station device.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－105612

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ｂ ３３０

審査請求　未請求　請求項の数４　ＯＬ　（全　９　頁）

(21)出願番号　特願平8－260757

(22)出願日　平成８年(1996)10月１日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　中村　公治
大阪府大阪市中央区城見二丁目１番61号
富士通関西通信システム株式会社内

(72)発明者　江谷　為之
大阪府大阪市中央区城見二丁目１番61号
富士通関西通信システム株式会社内

(72)発明者　神田　恭典
大阪府大阪市中央区城見二丁目１番61号
富士通関西通信システム株式会社内

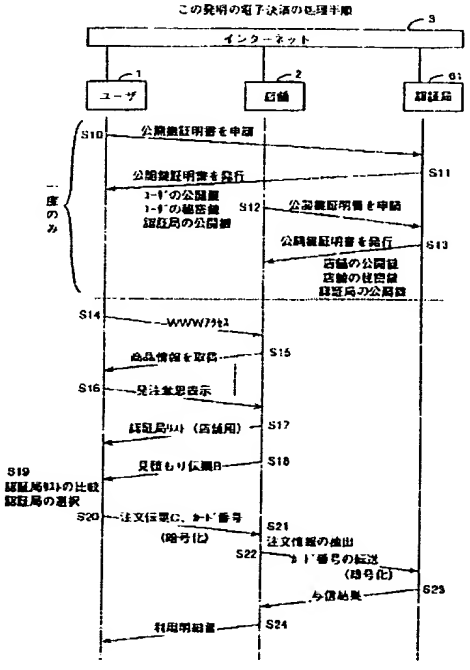
(74)代理人　弁理士　野河　信太郎

(54)【発明の名称】　認証システム

(57)【要約】

【課題】　この発明は、認証システムに関し、ユーザが利用可能な認証局が複数個ある場合でも、容易に利用する認証局を選択できる認証システムを提供することを課題とする。

【解決手段】　ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決裁の認証システムにおいて、クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決裁を行うことを特徴とする。



ユーザと店舗で同じブランドを
見つけ、そのブランドを選択して
決裁を行う

1

【特許請求の範囲】

【請求項１】　ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決裁の認証システムにおいて、

クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決裁を行う認証システム。

【請求項２】　前記サービス提供サーバが、サーバの所有者が契約している認証局のリストを作成する第１の作成手段と、この作成された認証局のリストを前記クライアント装置へ送信する第１の送信手段とを備え、

前記クライアント装置が、前記第１の送信手段によって送信された認証局のリストを受信する第１の受信手段と、

クライアント装置のユーザが契約している認証局のリストを作成する第２の作成手段と、

ユーザの契約している認証局が発行した鍵を記憶する鍵記憶手段と、

前記第１の受信手段によって受信された認証局のリストと前記第２の作成手段によって作成された認証局のリストとを比較して共通する認証局を選択する比較手段と、

前記比較手段によって選択された認証局が発行した鍵であって、かつ前記鍵記憶手段に記憶されている鍵を用いて電子決裁情報を暗号化する暗号化手段と、

暗号化された電子決裁情報をサービス提供サーバへ送信する第２の送信手段とを備えることを特徴とする請求項１記載の認証システム。

【請求項３】　前記サービス提供サーバが、

前記クライアント装置から送信された電子決裁情報を受信する第２の受信手段と、

受信した電子決裁情報を復号化する復号化手段と、

復号化された電子決裁情報を用いて受注処理を行う受注手段とをさらに備えることを特徴とする請求項２記載の認証システム。

【請求項４】　前記クライアント装置が、前記第２の作成手段によって作成された認証局のリストに含まれる複数の認証局に選択優先度を付与する優先度付与手段をさらに備え、

前記比較手段が選択した共通の認証局が複数個存在する場合に、選択優先度の最も高い共通の認証局のみを抽出することを特徴とする請求項２記載の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、認証システムに関し、特にネットワークを利用した取引や売買、サービスの授受を実現する場合に必要となる、電子決裁上の認証を行う認証システムに関するものである。最近、インターネットの World Wide Web（以降ＷＷＷと称する）を利用して、ネットワーク上の取引（電子ショッピングや電子商取引）が実現されつつある。このようなネットワーク上の取引では、商品又はサービスを提供する店舗・業者と消費者などのユーザは取引や売買を直接対面して行うことができない。したがって、ユーザの身元の保証と、サービスを提供する業者（電子ショッピングなら店舗）の身元保証をいかに行うかが、安全に取引や売買を行う上で大変重要である。

2

【０００２】

【従来の技術】クライアントーサーバ型の形態をとるネットワークを利用した電子商取引において、サーバ側からクライアント（ユーザ）の認証を行う場合、現状では公開鍵暗号方式をベースとした認証を行うのが一般化しつつある。すでに実用化されているクレジットカード決済では、ＳＥＴ（Secure Electronic Transactions）やＳＴＴ、ＳＥＰＰなどの電子決裁技術が有名である。

【０００３】電子決裁の一例として、ＳＥＴを用いた場合のクレジット決裁の従来例を以下に示す。図６は、ユーザ及び店舗の認証を行い、インターネットを利用してユーザがその店舗から商品を購入するクレジット決裁の手順を示したものである。ここで、ユーザ１０１、店舗１０２及び認証局１０３は、インターネット１００を経由して接続されているものとする。ユーザ１０１、店舗１０２及び認証局１０３には、それぞれパソコン等の端末にこのようなクレジット決裁をするのに必要なソフトウェアが組み込まれる。認証局１０３とは、クレジット決裁を利用するユーザ又は店舗等の利用者の身分を公正・中立な立場で電子的に証明する第三者的機関であり、たとえばクレジット会社がこの認証局（Certificate Authority）を運営している。

【０００４】認証局１０３は、一般的に次のような業務を行うものである。

１）利用者の身分を確認して、その登録・管理をすること。

２）利用者に「公開鍵証明書」を発行すること。

３）公開鍵とこれと対となる秘密鍵の生成、更新、利用者に公開鍵及び秘密鍵の配送をすること。

４）否認防止のための発信及び受信の証明と内容の証明をすること。

５）通信目録の作成，鍵のコピーの管理及び再発行，これらの記録管理をすること。

【０００５】ここで「公開鍵証明書」とは、利用者（公開鍵の持主）の電子的な身分証明書である。この中には、利用者を特定するための名前などの登録情報，利用者に与えられる公開鍵が含まれ，認証局自身の秘密鍵によるデジタル署名が付与されている。このデジタル署名が付与されているため，「公開鍵証明書」は，利用者でない他者が公開鍵証明書を偽造することはできない構造となっている。

【０００６】したがって、以下に述べるような従来のクレジット決裁の手順を実行するためには、ユーザ１０１と店舗１０２とが同じ認証局からそれぞれの公開鍵の証明書を発行してもらっていることが必要である。

【０００７】図６において、Ｓ１００からＳ１０３の手順は、郵送等のオフライン手段を使用して行われる。すなわち、ユーザ１０１及び店舗１０２は、認証局１０３に自己の公開鍵を発行してもらうために、書類の郵送等により「公開鍵証明書」の申請を行う（Ｓ１００，Ｓ１０２）。この申請を受理した認証局１０３は、書類審査などで身元の確認を行った後、ユーザ１０１及び店舗１０２に対して「公開鍵証明書」を郵送する（Ｓ１０１，Ｓ１０３）。

【０００８】「公開鍵証明書」を受理したユーザ１０１及び店舗１０２は、クレジット決裁を実行するために、「公開鍵証明書」に記載されている情報及び対となる秘密鍵をそれぞれクレジット決裁を実行するパソコンに入力しておく。たとえば、ユーザから送信される情報を暗号化するために公開鍵証明書と秘密鍵が入力され、パソコンのハードディスク等に記憶される。

【０００９】Ｓ１０４からＳ１１１が、従来行われているクレジット決裁によって実際に商品購入を行う処理である。まず、ユーザ１０１が、インターネット１００を経由して、店舗１０２のＷＷＷブラウザにアクセスする（Ｓ１０４）。

【００１０】そして店舗１０２は、アクセスのあったユーザ１０１に対してその店舗１０２の所有する商品情報などを送信する（Ｓ１０５）。その後、商品情報を取得したユーザ１０１は、自己の望む商品が決定したら、発注意思表示のデータを店舗１０２へ送る（Ｓ１０６）。そして店舗１０２は、この発注意思表示に対して見積もり伝票をユーザ１０１へ送信する（Ｓ１０７）。見積もり伝票を受理したユーザ１０１は、必要な数量などを記入した発注伝票とクレジットカード番号等を店舗１０２へ送信する（Ｓ１０８）。店舗１０２は、発注情報のみを抽出して、残りのクレジットカード番号など認証に必要な情報を認証局１０３へ転送する（Ｓ１０９）。認証局１０３では、この決裁に必要な情報を確認後、認証が完了したか否かを示す与信結果を店舗１０２へ返信する（Ｓ１１０）。与信結果を受信した店舗１０２では、認証が正常に完了した場合には、利用明細書をユーザ１０１へ送信する（Ｓ１１１）。以上によってクレジット決裁による商品購入が完了する。ただし、ユーザの契約している認証局と店舗の契約している認証局が異なる場合などは、認証が正常に行えないため、認証不可の与信結果が送信され、クレジット決裁は成立しない。

【００１１】

【発明が解決しようとする課題】従来、このようなネットワークを介した電子的なクレジット決裁を利用せずに、ユーザが店舗に出向いて「クレジットカード」の現物を店舗に提示してクレジット決裁をする場合にも、ユーザ及び店舗の双方が同じクレジット会社と契約していることが前提となっている。同様に、前記したネットワークを介した電子的なクレジット決裁でも、ユーザ及び店舗の双方が同じクレジット会社と契約していることが前提となる。すなわち、前記したようなどんな電子決裁や認証を用いたとしても、ユーザも店舗もある認証局と個別に契約を結ばなければならない。

【００１２】認証局が一つしか存在しない場合には、必ずユーザと店舗が同じ認証局による認証を受けるので問題とはならないが、複数の認証局が存在する場合には、ユーザと店舗が契約を結ぶ認証局が異なる場合があるので、クレジット決裁が不可能な場合があり得る。現実には、クレジット会社は複数社存在するので、クレジット会社が運営する認証局も複数存在しうる。したがって、ユーザも、店舗も複数のしかも任意の認証局と契約しているという状態が想定される。このような状態において、ユーザがクレジット決裁を行おうとする場合は、次のような問題点が発生する。

【００１３】１）ユーザが購入したい商品を販売している店舗が契約している認証局が、そのユーザが契約している認証局の中に含まれているか否かを、ユーザが常に確認する必要がある。

２）また、店舗が契約している認証局は一般に異なるため、購入する店舗を変更する場合には、その都度店舗が契約している認証局をユーザが確認する必要がある。

３）クレジット会社が認証局を運用すれば、クレジット会社の認証利用特典などのために、ユーザは電子取引にて利用可能な認証局のうち、自分の好みの認証局を選択する煩わしさが発生する。

【００１４】この発明は以上のような事情を考慮してなされたものであり、上記３つの問題点を解決することを課題とし、ユーザが複数の認証局と契約している場合にも、ユーザが容易に認証局を選択することのできる認証システムを提供するものである。

【００１５】

【課題を解決するための手段】この発明は、ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決裁の認証システムにおいて、クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決裁を行う認証システムを提供するものである。

【００１６】また、サービス提供サーバが、サーバの所有者が契約している認証局のリストを作成する第１の作成手段と、この作成された認証局のリストを前記クライアント装置へ送信する第１の送信手段とを備え、前記クライアント装置が、前記第１の送信手段によって送信さ

5

れた認証局のリストを受信する第1の受信手段と、クライアント装置のユーザが契約している認証局のリストを作成する第2の作成手段と、ユーザの契約している認証局が発行した鍵を記憶する鍵記憶手段と、前記第1の受信手段によって受信された認証局のリストと前記第2の作成手段によって作成された認証局のリストとを比較して共通する認証局を選択する比較手段と、前記比較手段によって選択された認証局が発行した鍵であって、かつ前記鍵記憶手段に記憶されている鍵を用いて電子決裁情報を暗号化する暗号化手段と、暗号化された電子決裁情報をサービス提供サーバへ送信する第2の送信手段を提供するものである。

【0017】さらに、前記サービス提供サーバが、前記クライアント装置から送信された電子決裁情報を受信する第2の受信手段と、受信した電子決裁情報を復号化する復号化手段と、復号化された電子決裁情報を用いて受注処理を行う受注手段を備えてもよい。ここで、前記クライアント装置が、前記第2の作成手段によって作成された認証局のリストに含まれる複数の認証局に選択優先度を付与する優先度付与手段をさらに備え、前記比較手段が選択した共通の認証局が複数個存在する場合、選択優先度の最も高い共通の認証局のみを抽出するようにしてもよい。

【0018】ネットワークの対象としては、世界中の各種サーバ、パソコン等が多数接続されるという点で見れば、インターネットが最も好ましいが、これに限定されるものではなく、その他のWAN、LAN等であってもよい。クライアント装置は、ネットワーク接続機能を有したパソコンやワークステーションを用いることができる。サービス提供サーバは、主として店舗，営業所等に設置され、提供するサービスの規模に応じてワークステーションやパソコンを用いればよい。

【0019】この発明で対象となる認証局のリストは、「クライアント装置側のユーザ、すなわち購買者が契約した認証局」のリストと、「サービス提供サーバ側の所有者、すなわち業者・店舗が契約した認証局」のリストの2種類がある。

【0020】認証局とは、たとえばクレジット会社をさし、ユーザ及び店舗の身元を電子的手段を用いて認証する機能を有するものである。ここでも、この認証機能を実行する装置は、通常パソコンやワークステーションなどのコンピュータが利用され、認証に必要なデータは厳格な管理下におかれる。したがって認証局としては、クレジット会社自体の他、公的機関あるいは、信頼のおける第三者機関が運営する場合もある。

【0021】以上、述べたクライアント装置，サービス提供サーバの各手段の機能は、通常、パソコン等に内蔵されたソフトウェアと、CPUを中心とするハードウェアによって制御される。また、クライアント装置及びサービス提供サーバとも、マンマシンインタフェースとして、キーボード等の入力装置，CRT，プリンタなどの出力装置を備えることが好ましい。

6

【0022】電子決裁を行う場合に、クライアント装置とサービス提供サーバ間を転送される電子決裁情報は、通常安全のため暗号化される。この暗号化のために、一般的に認証局が発行する「鍵」と呼ばれるデータが用いられる。この鍵として、たとえば、1組の「公開鍵」と「秘密鍵」を用いる方法がある。

【0023】

【発明の実施の形態】以下、図面に示す実施の形態に基づいてこの発明を詳述する。なお、これによってこの発明が限定されるものではない。図1は、この発明の認証システムの基本構成ブロック図である。ユーザ装置1は、ユーザ側に設置される装置であり、たとえばパーソナルコンピュータ（パソコン）のような装置である。店舗装置2は、店舗側に設置される装置であり、商品やサービスを提供するサーバである。認証局装置61，62……6nは、たとえばクレジット会社が運営する装置であり、公開鍵の発行や管理を行う装置である。

【0024】ユーザ装置1，店舗装置2，認証局装置（61……6n）は、インターネット3に接続され、インターネットの汎用通信プロトコルを実行するためのハードウェアとソフトウェアを備える。また、ユーザ装置1及び店舗装置2は、通信される情報の表示，入力，出力等のために、WWWブラウザ11，21を備えることが好ましい。

【0025】ユーザ装置1は、店舗装置2から送られてくる情報をWWWブラウザ11を介して表示し、ユーザからの入力によって発注処理を行う発注処理部12を備える。一方、店舗装置2は、ユーザから送られてくる発注情報を解析して受注処理を行う受注処理部22を備える。

【0026】各認証局装置61，62，……6nは、契約をかわしたユーザ及び店舗に対してそれぞれ独立した公開鍵を発行する。したがって、あるユーザが2つの認証局61，6nと契約をした場合は、そのユーザは、2つの公開鍵を持つことになる。同様に店舗が複数の認証局と契約した場合には、その複数個分の公開鍵を持つことになる。ユーザと店舗とが共通の認証局CAと契約していて、その認証局CAが発行したユーザ及び店舗の公開鍵を利用することによって電子決裁が成立する。

【0027】図1の認証局リスト13，23は、ユーザ又は店舗がそれぞれ契約している認証局に関する情報を記憶したものである。2つの認証局61，62と契約したユーザ装置1に記憶される認証局リスト（客用）13には、認証局61および62を識別する情報と、この2つの認証局が発行したそのユーザを特定するための「公開鍵証明書」が少なくとも含まれる。たとえば、認証局リスト（客用）13には、ユーザ識別コード番号，ユーザの公開鍵，その公開鍵を発行した認証局の識別番号

認証局のデジタル署名データが含まれる。認証局リスト（店舗用）２３には、店舗識別コード番号，店舗の公開鍵，その公開鍵を発行した認証局の識別番号，認証局のデジタル署名データが含まれる。

【００２８】発注処理部１２及び受注処理部２２は，通常ＣＰＵ，ＲＯＭ，ＲＡＭ，タイマー，Ｉ／Ｏコントローラなどからなるマイクロコンピュータから構成され，認証局リスト１３，２３は，不揮発性のメモリ，たとえばハードディスクに記憶される。

【００２９】以上のような基本構成を持つこの発明の認証システムは，ネットワークを介してユーザがある店舗に対して発注処理を実行した際に，ユーザ自らが同じ認証局と契約している店舗か否かを確認する操作をすることなしに，２つの「認証局リスト」１３，２３を利用して互いに共通な認証局を検索して，その共通の認証局を通した電子決裁を行なおうとするものである。

【００３０】図２に，この発明の一実施例における発注処理部１２及び受注処理部２２の詳細な構成ブロック図を示す。ここで示した各手段は，ロジック回路や専用ＬＳＩを用いてハードウェア的に独立した構成としてもよいが，一般的に，拡張性等の点からマイクロコンピュータと各手段に対応したプログラムを組合わせて，各手段の機能を実行させるようにすることが好ましい。

【００３１】また，認証局リスト１３，２３，注文伝票１９及び見積もり伝票３０，その他各手段が実行するのに必要なデータは，ＲＡＭやハードディスクなどに記憶される。ＷＷＷブラウザ１１，ＷＷＷサーバ２１は，インターネットにアクセスしてＷＷＷの情報を表示，転送できるソフトウェアであればよく，市販されているソフトウェアを用いればよい。

【００３２】ここで，認証局リスト１３，２３は，ユーザ又は店舗が契約した認証局から「公開鍵証明書」を受理したときに，ユーザ又は店舗の担当者がキーボード等を用いて必要なデータを入力することによって予め作成される。「公開鍵証明書」がフロッピーディスクなどの記憶媒体に入れられて発行される場合には，そのフロッピーディスクをユーザ又は店舗のパソコンに挿入し，所定の操作を行って自動的にデータを読み取って認証局リスト１３，２３を生成するようにしてもよい。

【００３３】また，新たな認証局と契約した場合には，その都度その新たな認証局発行の「公開鍵証明書」に記載されたデータを入力することによって，認証局リスト１３，２３は更新される。すなわち，新たな認証局の情報が認証局リスト１３，２３に追加される。

【００３４】店舗装置２の受注処理部２２において，認証局リスト作成手段２７は店舗が契約する認証局の一覧である認証局リスト（店舗用）２３を作成し，データ受信手段２６はＷＷＷサーバ２１から中継された注文伝票Ｃを復号化手段２５に引き渡すものである。

【００３５】復号化手段２５は，注文伝票Ｃに添付されたユーザの公開鍵を基に注文伝票を復号化し平文の注文内容を得，これを受注手段２９に引き渡す。受注手段２９は平文の注文内容に応じて受注処理を行う。ここで，受注処理には，ユーザの確認のため，認証局との間で行われる与信処理が含まれる。

【００３６】伝票作成手段２８は，ＷＷＷブラウザ２１からの中継されたユーザからの注文内容に応じて，見積もり伝票Ｂを作成するものである。データ送信手段２４は，認証局リスト（店舗用）２３等をＷＷＷサーバ２１へ送るものである。ＷＷＷサーバ２１は，ＷＷＷブラウザ１１から送信された要求データに応答して，商品情報の送信，見積もり伝票Ｂの送信，認証局リスト（店舗用）２３等の送信を行うものである。

【００３７】ユーザ装置１は，ＷＷＷブラウザ１１と発注処理部１２からなる。ＷＷＷブラウザ１１は，店舗装置２から送られてきた認証局リスト（店舗用）２３と見積もり伝票Ｂを発注処置部１２に中継するものである。発注処理部１２において，認証局リスト作成手段１８はユーザが契約する認証局の一覧である認証局リスト（客用）１３を作成し，データ受信手段１４はＷＷＷブラウザ１１から中継された認証局リスト（店舗用）２３を認証局リスト比較手段１５に，見積もり伝票Ｂを暗号化手段１６に引き渡すものである。

【００３８】認証局リスト比較手段１５は，認証局リスト（客用）１３と認証局リスト（店舗用）２３を比較し，ユーザと店舗に共通な認証局ａを決定する。暗号化手段１６は，決定された認証局ａの管理するこのユーザ固有の秘密鍵により注文内容を暗号化し，認証局ａの発行する公開鍵を添付して注文伝票Ｃを作成し，注文伝票Ｃの送信データ送信手段１７に依頼する。データ送信手段１７は，注文伝票Ｃを店舗装置２に送信するものである。

【００３９】図３に，この発明の一実施例における電子決裁の処理手順の説明図（シーケンス図）を示す。ステップＳ１０からＳ１３までの処理は，従来におけるステップＳ１００からＳ１０３までの処理と同じであり，ユーザ１及び店舗２とも郵送等のオフライン手段によって認証局６１から発行される「公開鍵証明書」を事前に取得する。ここで，ステップＳ２２までの電子決裁が完了するためには，ユーザ１と店舗２とが少なくとも１つの共通の認証局と契約を結び，その認証局から発行された「公開鍵証明書」を取得する必要がある。

【００４０】ステップＳ１１，Ｓ１３において「公開鍵証明書」が認証局から発行されるが，これには，通常この認証局の公開鍵が含まれる。含まれない場合は，たとえば別郵送にて発行してもよい。また，これとは別に，ユーザ１に対しては，認証局６１が作成したユーザ１の秘密鍵が，店舗２に対しては，認証局６１が作成した店舗２の秘密鍵が，その認証局から郵送等のオフライン手段によって発行される。ただし，この秘密鍵は，ユーザ

又は店舗が厳密に管理すべきものなので、認証局が発行する形態をとらずに、ユーザ又は店舗自身のプログラムで自動生成するようにしてもよい。

【００４１】なお、「公開鍵証明書」のフォーマットは、ＩＴＵ－ＴのＸ．５０９で規定されたものを用いればよい。以上のステップＳ１０からステップＳ１３までのオフライン処理は、この認証システムを運用する上で前提となる処理であり、この手段を一回のみ行なえばよい。

【００４２】ステップＳ１４において、ユーザ１が、インターネット３を経由して、店舗２のＷＷＷサーバ２１にアクセスする。ステップＳ１５において、店舗２が、このユーザ１に対してその店舗２の所有する商品情報等を送信する。ステップＳ１６において、この商品情報を取得したユーザ１は、自己の望む商品あるいはサービスが決定したら、「発注意思表示」を示すデータを店舗２へ転送する。ここまでの処理は、図２におけるＷＷＷブラウザ１１、ＷＷＷサーバ２１間の通信によって実行することが可能であり、転送されるデータは図２には図示していないが、ユーザ１及び店舗２の各装置中のハードディスク等にデータベースとして蓄積しておけばよい。

【００４３】ステップＳ１７において、店舗２では、この発注意思表示に対して、認証局リスト作成手段２７によって作成されたこの店舗２が契約しているすべての認証局を含む認証局リスト（店舗用）２３を、データ送信手段２４を通してＷＷＷサーバ２１がユーザ１へ送信する。ユーザ１では、この認証局リスト（店舗用）２３は、ＷＷＷブラウザ１１で中継され、データ受信手段１４によって受信される。

【００４４】ステップＳ１８において、さらに店舗２では、伝票作成手段２６が見積もり伝票Ｂ３０を作成し、データ送信手段２４を通してＷＷＷサーバ２１がこの見積もり伝票Ｂ３０を送信する。ユーザ１では、同様にしてこの見積もり伝票Ｂ３０がデータ受信手段１４によって受信されると、図示していない表示手段あるいは印刷手段等を利用してユーザに見積もり内容が提示される。

【００４５】ステップＳ１９において、ユーザ１で予め作成されていたユーザの認証局リスト（局用）１３と、ステップＳ１７で受信された認証局リスト（店舗用）２３とを、認証局リスト比較手段１５が比較し、電子決裁をするための認証局を選択する。

【００４６】ここで、認証局リスト１３及び２３には、認証局の名称あるいは識別番号が含まれているので、両リストに同じものが含まれているかどうかを判断する。両リストに同じものが含まれていない場合には、電子決裁に必要な認証ができないことになり、残念ながら、この電子決裁は不成立となり、ユーザは商品等を購入できない。一方、両リストに一つでも同じ認証局が含まれている場合は、認証が可能であるため、この両リストに共通な認証局を選び出す。

【００４７】共通の認証局が複数存在する場合には、その中から適当な一つを選べばよい。あるいは、複数の認証局を表示手段に表示して、ユーザに選択させるようにしてもよい。さらに後述するように、予め付与された選択優先度によって自動選択するようにしてもよい。

【００４８】ステップＳ２０において、認証を行う認証局が選択されれば、暗号化手段１６が、ユーザを特定するカード番号及び選択された認証局の識別番号を含む注文伝票Ｃ１９を暗号化して、データ送信手段１７がＷＷＷブラウザ１１を介してこれらの暗号化された情報を店舗２へ送信する。このとき、暗号化には、ユーザ固有の秘密鍵や選択された認証局の公開鍵が使用される。

【００４９】たとえば、ユーザを特定するカード番号は、認証局がユーザの身元が正しいかどうかを確認するものであるので、選択された認証局の公開鍵（ステップＳ１１で発行されたもの）で暗号化すればよい。また、カード番号を除く注文伝票の情報、たとえば商品名，番号，数量，金額などは、店舗２が受注する際に必要となるものであるので、ユーザ固有の秘密鍵で暗号化すればよい。また、店舗２でこの暗号化された情報を解くために、ユーザの公開鍵も、通常、注文伝票の送信時に、ユーザ１から店舗２へ送信される。

【００５０】ステップＳ２１において、店舗２のデータ受信手段２６が注文伝票Ｃを受信した後、復号化手段２５が「カード番号」を除いた注文に関与する情報のみを抽出して復号化を行なう。この情報の復号化には、通常、送信されてきたユーザの公開鍵が用いられる。この復号化された情報は、受注手段２９へ渡され、商品手配などの受注処理が実行される。

【００５１】一方、店舗２において、ユーザの「カード番号」は、データ送信手段２４によって認証局６１へ送られる（ステップＳ２２）。ここでの認証局６１は、ユーザ１が選択した認証局であることは言うまでもない。また、「カード番号」は、まだ認証局６１の公開鍵で暗号化されたままである。

【００５２】ステップＳ２３において、認証局６１に送られてきたユーザの「カード番号」は、認証局６１の秘密鍵を用いて復号化される。そして、認証局６１は、ユーザの身元を認証した後、認証の可否（与信結果）を店舗２へ通知する。ステップＳ２４において、この与信結果を受けた店舗２は、ユーザ１の認証が正常にできたと判断した場合には、利用明細書をユーザ１へ送信する。以上のようにして、この発明の一実施例の電子決裁が完了する。

【００５３】ステップＳ２０の暗号化には、現状では、ＲＳＡの公開鍵方式が最も広く使われているため、ＲＳＡの公開鍵方式を用いるのが好ましいが、ＲＳＡ以外の公開鍵方式（例えば、ＢＯＳや楕円方式等）でも可能である。また、公開鍵方式だけでなく、公開鍵方式と共通鍵方式（例えば、ＦＥＡＬやＭＵＬＴ１２、ＭＩＳＴ

11

Y）と組み合わせた方式でも可能である。また、注文伝票を送信する方法としては、暗号化された伝票を電子メールで送る方法でもよい。

【００５４】このように、ユーザも店舗も、複数の認証局と契約していた場合に、店舗側が契約しているすべての認証局のリストをユーザに通知するようにしているので、ユーザが、その店舗がどの認証局と契約しているかを確認する操作をすることなく、容易に電子決裁を行う認証局を選択することが可能となる。

【００５５】この発明において、店舗側とユーザ側で同一の認証局と契約を結び、どちらも同じ認証局から発行される公開鍵証明書を事前に取得する電子決裁の形態を実施例として説明した。しかし、世界的にも電子決裁（電子商取引）はまだ実験段階であり、認証の方法はさまざまな形態が考えられる。また、実際の認証局の運営をクレジット会社が行う形態をとる場合には、当面は認証局が複数存在する可能性がある。このような場合に、特にこの発明の認証システムは有効に機能する。

【００５６】図４、及び図５に、この発明の認証局リストの一実施例を示す。図４は、ユーザ装置１で作成される認証局リスト（客用）１３の実施例である。図５は、店舗装置２で作成される認証局リスト（店舗用）２３の実施例である。いずれも認証局を示す識別番号（ａ，ｂ，……ｇ）と、暗号化された各認証局が発行した「公開鍵証明書」の内容から構成される。

【００５７】ここで、前記したステップＳ１９では、認証局リスト比較手段１５は、両リストの認証局の識別番号の中に一致するものがあるか否かを判断すればよい。また、図４に示すように、認証局リスト（客用）１３には、選択優先度を付与してもよい。たとえば、認証局ａの選択優先度を高く、認証局ｃの選択優先度を低くなるように数字を付与してもよい。図４では、ユーザが契約した認証局のうち、認証局ａが最も選択優先度が高く、次に認証局ｄが高く、認証局ｃが最も選択優先度が低い。図４と図５を比較すると、両リストに共通する認証局は、“ｃ”と“ｄ”であることがわかる。

【００５８】したがって、このリストの場合は認証局“ｃ”又は“ｄ”が選択されることになるが、複数の認証局が選択可能な場合は、最初に見つかった方を選択してもよい。また、選択優先度の最も高いものを優先して選ぶことにすると、図４のような優先度を付与した場合、認証を行う認証局としては、優先度の高い“ｄ”の方が自動的に選択されることになる。なお、この選択の優先度付けは、ユーザが認証局リスト（客用）１４を作成する際に、キーボード等の入力手段を利用して行なえばよい。

【００５９】このように、予めユーザの契約した認証局に選択優先度を付与しておけば、電子決裁で利用可能な認証局が複数存在する場合でも、自動的に利用する認証局が一つ選択される。したがって、ユーザがその都度利用する認証局を指定する必要がなくなるので、ユーザにとってスムーズな電子決裁手続をすることができる。

12

【００６０】なお、上記の実施例では、ユーザ，店舗及び認証局がインターネットを介して接続された場合を示したが、この発明の認証システムは、他のＷＡＮやＬＡＮなどのネットワークでも実施できる。他のネットワークの場合には、通信プロトコルやデータフォーマットの形式をそのネットワークで規定されたものを使えばよく、図２に示した構成及び図３に示した処理手順はそのまま利用することができる。

【００６１】

【発明の効果】この発明によれば、サービス提供サーバからクライアント装置へ、サービス提供サーバが契約している認証局のリストを送信するようにしているので、クライアント装置において、ユーザの契約している認証局とサービス提供サーバの契約している認証局とを比較して、利用する認証局を選択することができる。また、クライアント装置においてユーザが契約している認証局に選択優先度を付与するようにしているので、ユーザは、複数の認証局の中から利用する認証局をその都度選択する必要はなく、スムーズに電子決裁を行うことができる。

【図面の簡単な説明】

【図１】この発明の基本構成ブロック図である。

【図２】この発明の一実施例における構成ブロック図である。

【図３】この発明の一実施例における電子決裁の処理手順の説明図である。

【図４】この発明の認証局リスト（客用）の実施例を示す図である。

【図５】この発明の認証局リスト（店舗用）の実施例を示す図である。

【図６】従来の電子決裁の処理手順の説明図である。

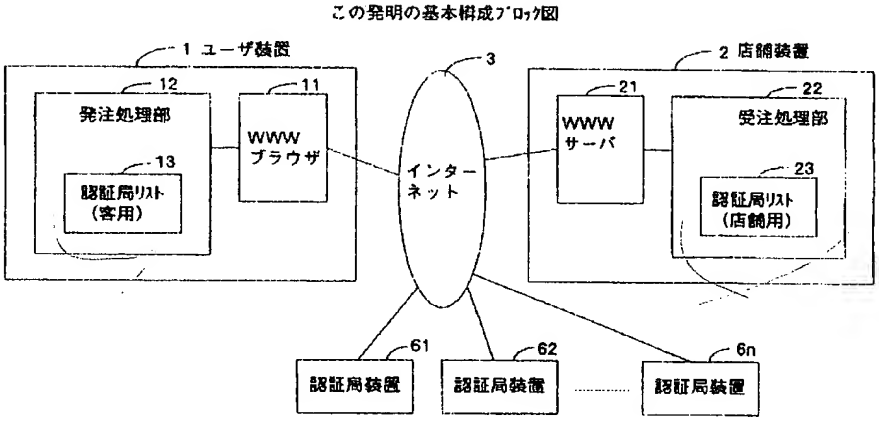
【符号の説明】

１　ユーザ装置
２　店舗装置
１１　ＷＷＷブラウザ
１２　発注処理部
１３　認証局リスト（客用）
１４　データ受信手段
１５　認証局リスト比較手段
１６　暗号化手段
１７　データ送信手段
１８　認証局リスト作成手段
１９　注文伝票Ｃ（カード番号）
２１　ＷＷＷサーバ
２２　受注処理部
２３　認証局リスト（店舗用）
２４　データ送信手段
２５　復号化手段

13　　14

２６　データ受信手段
２７　認証局リスト作成手段
２８　伝票作成手段
＊２９　受注手段
３０　見積もり伝票Ｂ
＊

【図１】

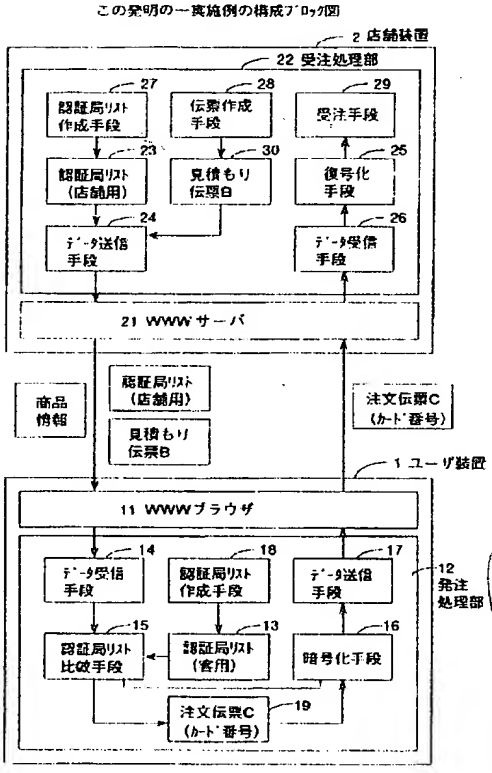


【図５】

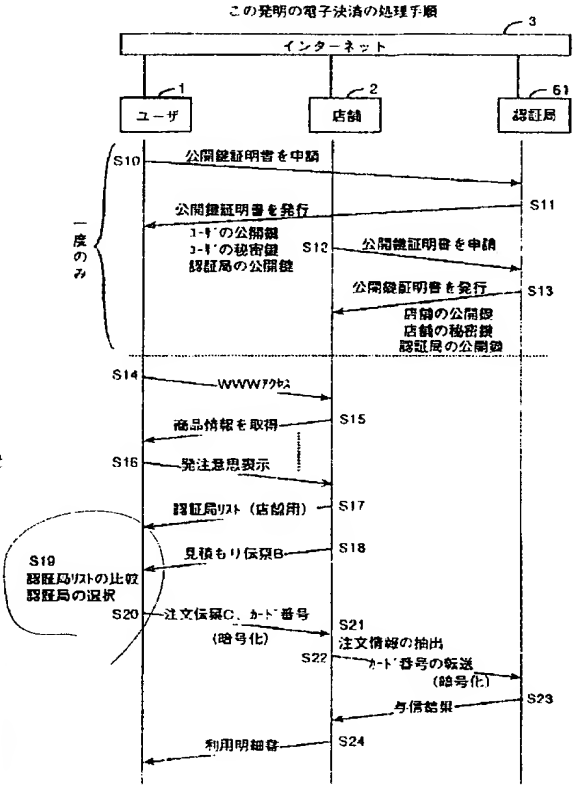
この発明の認証局リスト（店舗用）

認証局	証明書（暗号化）
b	公開鍵証明書（b局発行）
c	公開鍵証明書（c局発行）
d	公開鍵証明書（d局発行）
e	公開鍵証明書（e局発行）
f	公開鍵証明書（f局発行）
g	公開鍵証明書（g局発行）

【図２】



【図３】



【図４】

この発明の認証局リスト（客用）

優先度	認証局	証明書（暗号化）
大 1	a	公開鍵証明書（a局発行）
2	d	公開鍵証明書（d局発行）
小 3	c	公開鍵証明書（c局発行）

【図６】